

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problems Mailbox.**

**THIS PAGE BLANK (USPTO)**

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-231595

(43)Date of publication of application : 22.08.2000

(51)Int.Cl.

G06F 19/00

G06K 17/00

G07F 19/00

G07F 7/08

(21)Application number : 11-032793

(71)Applicant : NIPPON TELEGR & TELEPH  
CORP <NTT>

(22)Date of filing : 10.02.1999

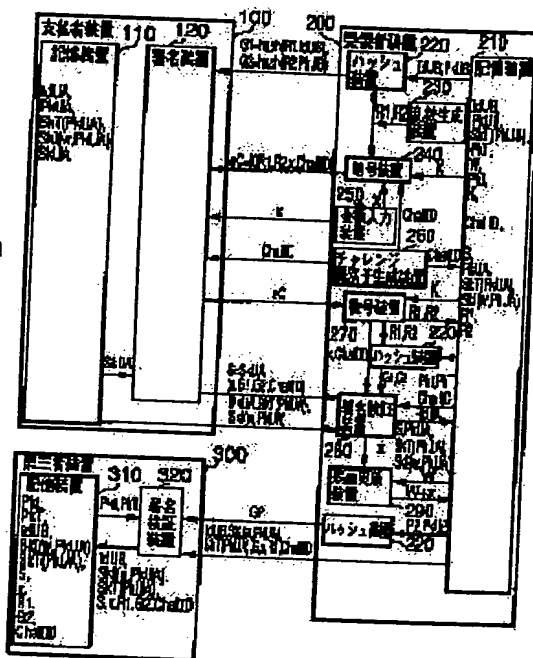
(72)Inventor : TORAMATSU KOICHI  
MORIHATA HIDEMI

(54) METHOD AND DEVICE FOR TRANSFERRING IC CARD ELECTRONIC MONEY  
AND ITS PROGRAM RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To certify IC card balance to the third person when an IC card is damaged.

SOLUTION: A recipient calculates a random number R1, the hash value G1 of a recipient identifier IdUB, a random number R2 and the hash value G2 of a recipient public key, makes a value eC obtained by enciphering R1, R2, a received amount (x) and a challenge identifier ChallID with a key K, sends G1, G2, eC, (x), and ChallID to a payer, and the payer generates a signature S for reception information with a secret key and sends the recipient S, the signature SkT (PkUA) of an authentication institution of a payer public key PkUA and an issuing institution signature SkI (w and PkUA) of the amount (w). The recipient verifies them, when all of them are satisfied, then updates balance W into (x+ W) and sends a recipient public key PkUB, SkI (w and PkUA), SkT (PkUA), S, (x) and ChallID to the third person, and the third person performs signature verification of received information and stores the received information when they are accepted.



LEGAL STATUS

**THIS PAGE BLANK (USPTO)**

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

**THIS PAGE BLANK (USPTO)**

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号  
特開2000-231595  
(P2000-231595A)

(43)公開日 平成12年8月22日(2000.8.22)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード(参考)	
G 0 6 F 19/00		G 0 6 F 15/30	3 5 0	3 E 0 4 0
G 0 6 K 17/00		G 0 6 K 17/00	R	3 E 0 4 4
G 0 7 F 19/00		G 0 6 F 15/30	J	5 B 0 5 5
7/08			3 6 0	5 B 0 5 8
		G 0 7 D 9/00	4 7 6	9 A 0 0 1
審査請求 未請求 請求項の数 7 O L (全 6 頁) 最終頁に続く				

(21)出願番号 特願平11-32793

(22)出願日 平成11年2月10日(1999.2.10)

(71)出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72)発明者 虎松 恒一

東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

(72)発明者 森島 秀実

東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

(74)代理人 100066153

弁理士 草野 卓 (外1名)

最終頁に続く

(54)【発明の名称】 ICカード型電子マネー譲渡方法、その装置、そのプログラム記録媒体

(57)【要約】

【課題】 ICカード破損時に、第三者にICカード残高を証明可能とする。

【解決手段】 受領者は乱数R1、受領者識別子IdUBのハッシュ値G1、乱数R2、受領者公開鍵のハッシュ値G2を求め、R1、R2、受領額x、チャレンジ識別子ChallengeIDを鍵Kで暗号化した値eCを作り、G1、G2、eC、x、ChallengeIDを支払者へ送り、支払者はその秘密鍵で受領情報に対する署名Sを生成し、S、支払者公開鍵PkUAの認証機関の署名SkT(PkUA)、金額wの発行機関署名SkI(w, PkUA)を受領者へ送る。受領者はこれらを検証し、全て合格で、残高Wをx+Wとし、支払者公開鍵PkUB、SkI(w, PkUA)、SkT(PkUA)、S、x、ChallengeIDを第三者へ送り、第三者は受信情報の署名検証を行い、合格で受信情報を保存する。

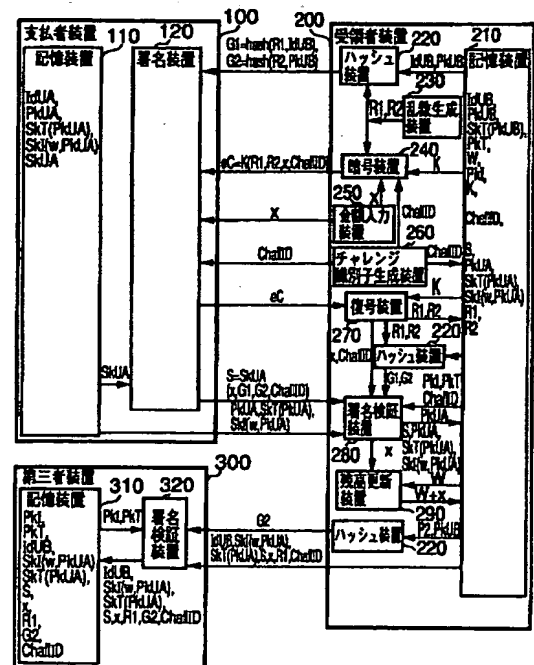


図 2

【特許請求の範囲】

【請求項1】 ICカードで現金価値を管理する電子マネーを譲渡する方法において、  
受領者装置が支払者装置から電子マネーを受領すると同時に、

第三者機関装置に譲渡に関する情報を送信し、  
その第三者機関装置はその受信した譲渡に関する情報を記憶装置に保存することを特徴とする電子マネー譲渡方法。

【請求項2】 受領者装置から受信したチャレンジ情報に対し支払者装置が署名をして受領者装置へ送信し、受領者装置が受信した署名を検証することにより支払いが行われる電子マネー譲渡方法において、  
受領者装置はチャレンジ情報を支払者装置に送信し、  
支払者装置はチャレンジ情報に対する署名（以下、支払者署名）を作成し、  
支払者署名を受領者装置に送信し、  
受領者装置は支払者署名がチャレンジ情報に対して正しく署名されている事を検証し、  
その検証に合格すると支払者署名を受領し、  
第三者機関装置に支払者署名およびその署名検証に必要な情報を送信し、  
第三者機関装置は支払者署名を保存することを特徴とする電子マネー譲渡方法。

【請求項3】 請求項2記載の方法において、  
上記支払者署名がチャレンジ情報に対して正しく署名されている事を検証し、  
検証に合格すると第三者機関装置にログ送信が可能であるかを問い合わせ、  
可能であれば支払者署名を受領し、  
その後第三者機関装置に支払者署名を送信することを特徴とする電子マネー譲渡方法。

【請求項4】 受領者装置から受信したチャレンジ情報に対し支払者装置が署名して受領者装置へ送り、受領者装置でその署名を検証することにより電子マネーによる支払いが行われる受領者装置であって、  
受領者識別情報、支払者公開鍵などを記憶した記憶手段と、  
チャレンジ情報を生成する手段と、  
そのチャレンジ情報を支払者装置へ送信する送信手段と、  
支払者装置から支払者署名を受信する受信手段と、  
支払者署名を検証する署名検証手段と、  
この検証に合格すると支払者署名を、上記記憶手段に記憶すると共に第三者機関装置へ送信する手段と、  
を具備することを特徴とする受領者装置。

【請求項5】 上記検証に合格すると、第三者機関装置にログ送信が可能であるかを問い合わせる手段と、  
ログ送信が可能である回答を受信すると、上記支払者署名の送信及び記憶手段への格納を行う手段と、

を具備する請求項4記載の受領者装置。

【請求項6】 受領者装置から受信したチャレンジ情報に対し支払者装置が署名して受領者装置へ送り、受領者装置でその署名を検証することにより電子マネーによる支払いが行われる受領者装置のコンピュータは、  
チャレンジ情報を生成する処理と、  
そのチャレンジ情報を支払者装置へ送信する処理と、  
支払者装置から支払者署名を受信する処理と、  
支払者署名を検証する処理と、  
この検証に合格すると支払者署名を、記憶手段に記憶すると共に第三者機関装置へ送信する処理と、  
を実行させるプログラムを記録した記録媒体。

【請求項7】 上記検証に合格すると、第三者機関装置にログ送信が可能であるかを問い合わせる処理と、  
ログ送信が可能である回答を受信すると、上記支払者署名の送信及び記憶手段への格納を行う処理と、  
を上記コンピュータに実行させるプログラムを上記プログラムを含むことを特徴とする請求項6記載の記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、電気通信システムやICカードのような記録媒体を利用して電子マネーを譲渡する方法及びその装置に関する。

【0002】

【従来の技術】電子マネーシステムはセンタ管理型と呼ばれるものとICカード管理型と呼ばれるものの2つに大きく分類される。前者ではネットワーク上の管理センタにより利用者の所持する現金価値が管理されるが、トラフィックの集中を招くという問題点がある。

【0003】一方ICカード管理型は、ICカード中に現金価値が存在するためトラフィックの問題が生じない。ICカード型電子マネーでは、利用者ICカードから商店サーバへの支払、利用者ICカード間で行われる譲渡、共に2ノード間で情報をやりとりする事で行っていた。

【0004】

【発明が解決しようとする課題】従来のICカード型電子マネーの譲渡方法では、第三者が譲渡電子マネーの流通を管理できない、さらにはICカード破損時にその残高を証明する事が出来ず、破損ICカードに格納されていた電子マネー分の現金価値を利用者に保証できなくなるという問題点があった。

【0005】上記問題はICカード発行体と電子マネー発行体が一致する場合において顕著な問題となる。

【0006】

【課題を解決するための手段】受領者装置が支払者装置からの電子マネーを受領後、第三者機関装置に支払者情報、受領者情報、金額情報を含むログを残す事で、第三者機関装置が譲渡電子マネーの流通を管理する事が可能



となる。さらに金融機関装置の情報とつきあわせれば、第三者機関装置が利用者のICカード残高を管理する事が可能となる。

【0007】「預入情報を解析する事で取引履歴が判明する方式」という制限はなく、広く一般の電子マネー方式に適用可能な手段である。又、受領者装置が電子マネーを受領する前に第三者機関装置に対してログ送信が可能か否かを問い合わせる事で、第三者機関装置が営業時間外であったなどの原因で、ログ送信が出来ない状態に陥る可能性を抑えられる。

【0008】

【発明の実施の形態】この発明のシステム構成は図1に示すように支払者装置100、受領者装置200、第三者装置300により構成される。

**実施例1** (図2参照)

支払開始前に予め、支払者は、正規の利用者であることを示す証として、支払者公開鍵PkUAに対する認証機関の署名SkT(PkUA)を入手し、電子マネーを所持している事を示す証として、金額w、および支払者公開鍵に対する電子マネー発行機関の署名SkI(w, PkUA)、つまりPkUAに対する金額wの電子マネーを入手し、これらを支払者装置100の記憶装置110に格納してある。

【0009】受領者は、認証機関の公開鍵PkTおよび発行機関の公開鍵PkIを入手し、秘密鍵Kを作成して保持し、これらを受領者装置200の記憶装置210に格納してある。支払い時に、受領者装置200は、乱数生成装置230より乱数R1、R2を生成し、受領者ID(以下、IdUB)と乱数R1のハッシュした値G1、および受領者公開鍵(以下、PkUB)と乱数R2のハッシュした値G2、をそれぞれハッシュ装置220で計算し、チャレンジ識別子生成装置260より、時刻などチャレンジを識別する値(以下、ChallengeID)を生成し、金額入力装置250より受領金額xを入力し、R1、R2、x、ChallengeIDを秘密鍵Kにより暗号装置240で暗号化した値eCを求め、G1、G2、eC、x、ChallengeIDを支払者装置100に送信する。

【0010】支払者装置100は、これらG1、G2、eC、x、ChallengeIDを受信すると、x、G1、G2、ChallengeIDに対する支払者署名Sを、支払者秘密鍵SkUAを使って署名装置120で作成し、S、eC、支払者公開鍵PkUA、SkT(PkUA)、SkI(w, PkUA)を受領者装置200に送信する。

【0011】受領者装置200はこれらを受信すると、eCをKにより復号装置270で復号化する事により、R1、R2、x、ChallengeIDを取出し、このR1、R2を用いてハッシュ装置220でIdUBとR1をハッシュしてG1を作成し、PkUBとR2をハッシュしてG2を作成する。署名検証装置280で、これらハッ

シュ値G1、G2と復号したx、ChallengeIDを用いてSがx、G1、G2、ChallengeIDに対する支払者署名になっている事をPkUAを使って確認し、SkT(PkUA)が正しい署名であることを、PkTを使って検証し、SkI(w, PkUA)が正しい署名であることを、PkIを使って検証し、全ての検証に合格した場合、保持していたChallengeIDを消去し、つまり支払者からの金額xの受領で不要となった情報を消去し、支払者装置100から受領したデータを保存し、残高更新装置290で残高をWからW+xへ更新し、R2、PkUBのハッシュ値G2をハッシュ装置220で計算し、IdUB、SkI(w, PkUA)、SkT(PkUA)、S、x、R1、G2、ChallengeID、つまりSとその署名・検証に必要な情報を第三者装置300に送信する。この送信情報中のIdUBとR1はこれらによりG1を作ってSの検証に用いることを可能としている。

【0012】第三者装置300は署名検証装置320で、SkT(PkUA)が正しい署名であることを、PkTを使って検証し、SkI(w, PkUA)が正しい署名であることを、PkIを使って検証し、全ての検証に合格した場合、IdUB、SkI(w, PkUA)、SkT(PkUA)、S、x、R1、G2、ChallengeIDをログとして記憶装置310に格納する。

【0013】このように第三者装置300には譲渡の経過を表わす情報が残されているから、電子マネー発行機関と第三者装置300が協力すれば、どのICカードにどれだけの残高があるかを、発行金額と譲渡金額とから知ることができる。なお1つのICカードに対し、複数の電子マネーが発行されることがあるから発行機関の協力が必要である。

**実施例2** (図3参照)

支払開始前に予め、支払者は、正規の利用者であることを示す証として、支払者公開鍵PkUAに対する認証機関の署名SkT(PkUA)を入手し、電子マネーを所持している事を示す証として、金額w、および支払者公開鍵PkUAに対する電子マネー発行機関の署名SkI(w, PkUA)を入手し、これらを記憶装置110に格納してある。

【0014】受領者は、認証機関の公開鍵PkTおよび発行機関の公開鍵PkIを入手し、秘密鍵Kを作成して保持し、これらを記憶装置210に格納してある。支払い時に、受領者装置200は乱数生成装置230より乱数R1、R2を生成し、受領者ID(以下、IdUB)と乱数R1のハッシュした値G1、および受領者公開鍵(以下、PkUB)と乱数R2のハッシュした値G2をそれぞれハッシュ装置220で計算し、チャレンジを識別する値(以下、ChallengeID)をチャレンジ識別子生成装置260で生成し、受領金額xを金額入力装置250から入力し、R1、R2、x、ChallengeIDを秘

密鍵Kで暗号化した値eCを暗号装置240で生成し、これらG1、G2、eC、x、ChallengeIDを支払者装置100に送信する。

【0015】支払者装置100は、G1、G2、eC、x、ChallengeIDを受信すると、x、G1、G2、ChallengeIDに対する支払者署名Sを署名装置120で支払者秘密鍵SkUAを使って作成し、S、eC、PkUA、SkT(PkUA)、SkI(w, PkUA)を受領者装置に送信し、受領者装置200は、これらを受信すると、eCをKにより復号装置270で復号化する事により、R1、R2、x、ChallengeIDを取出し、このR1、R2を用いてハッシュ装置220でIdUBとR1をハッシュしてG1を作成し、PkUBとR2をハッシュしてG2を作成する。署名検証装置280で、これらハッシュ値G1、G2と復号されたx、ChallengeIDを用いてSがx、G1、G2、ChallengeIDに対する支払者署名になっている事を確認し、SkT(PkUA)が正しい署名である事を、PkTを使って検証し、SkI(w, PkUA)が正しい署名である事を、PkIを使って検証し、全ての検証に合格した場合、第三者装置300にログ送信が可能かどうかを問い合わせ装置280により問い合わせ、可能であるとの返答を第三者装置300のサービス状態返答装置340から得た場合、保持していたChallengeIDを消去し、支払者装置100から受領したデータを保存し、残高をWからW+xへ残高更新装置290で更新し、IdUB、SkI(w, PkUA)、SkT(PkUA)、S、x、R1、G2、ChallengeIDを第三者装置300に送信する。

【0016】第三者装置300は署名検証装置320でSkT(PkUA)が正しい署名である事を、PkTを使って検証し、SkI(w, PkUA)が正しい署名である事を、PkIを使って検証し、全ての検証に合格した場合、IdUB、SkI(w, PkUA)、SkT(PkUA)、S、x、R1、G2、ChallengeIDをログとして記憶装置310に格納する。

【0017】上述において、R1、R2、x、ChallengeIDをKで暗号化する代りに、R1、R2、x、ChallengeIDをハッシュで攪乱して送信し、その返された

データをR1、R2、x、ChallengeIDで検証してもよい。あるいは受領者秘密鍵SkUBでR1、R2、x、ChallengeIDを署名し、その返されたデータを署名検証してもよい。このようにチャレンジ情報(x、R1、R2、ChallengeID)を支払者装置で改ざんされないように処理して支払者装置へ送る場合は、ChallengeIDのみを、支払者署名をもらうまで記憶しておけばその他のものは記憶しておく必要がなく、それだけ受領者装置の記憶装置として記憶容量が小さいものを使用できる。しかし、必ずしもそのようにすることなく、チャレンジ情報を受領者装置に、支払者署名をもらうまで保持すると共にチャレンジ情報をそのまま支払者装置へ送信してもよい。

【0018】

【発明の効果】従来のICカード型電子マネーの譲渡方法では、第三者が譲渡電子マネーの流通を管理したり、さらには破損ICカードに格納されていた電子マネー残高を確認し、利用者にその残高を保証したりする事が出来なかった。これに対し、この発明では、電子マネー譲渡に関する情報(支払者情報、受領者情報、金額情報)が第三者機関に残るため、金融機関の電子マネー発行情報とつきあわせれば、支払者、受領者の何れの利用者ICカードの残高を管理、保証する事が可能となった。譲渡ごとに第三者装置への通信分のトラフィック増加はあるが、この発明は商店への支払分のトラフィックには影響を与えないため、ICカード型のトラフィック軽減というメリットは継承している。

【0019】さらに受領者装置において、受領処理の前に第三者機関がサービス提供中であるかどうかを問い合わせる事によって、第三者機関が営業時間外などの理由でログ送信が不可能な状態に陥るのを抑える事が可能となった。

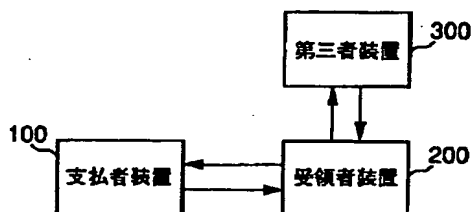
【図面の簡単な説明】

【図1】この発明の構成要素を示すブロック図。

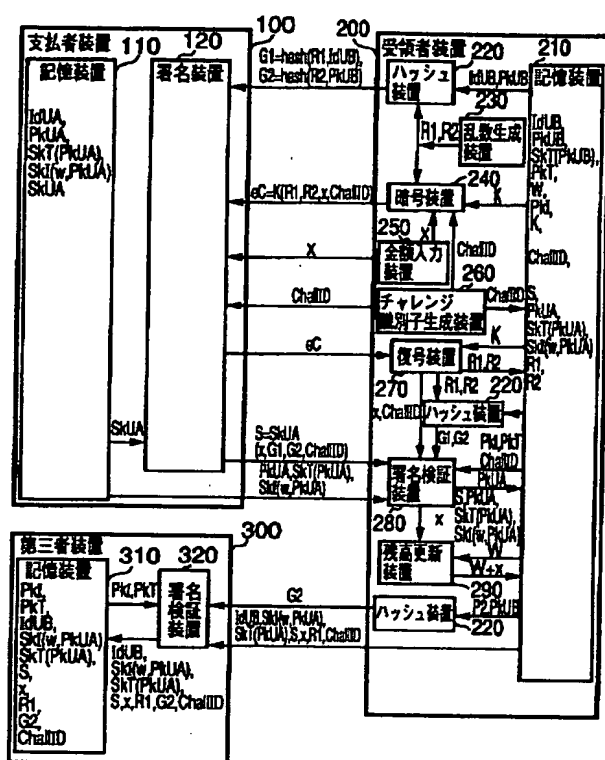
【図2】この発明の実施例1の受領処理を示すブロック図。

【図3】この発明の実施例2の受領処理を示すブロック図。

【图 1】



【図2】



**2**

【図3】

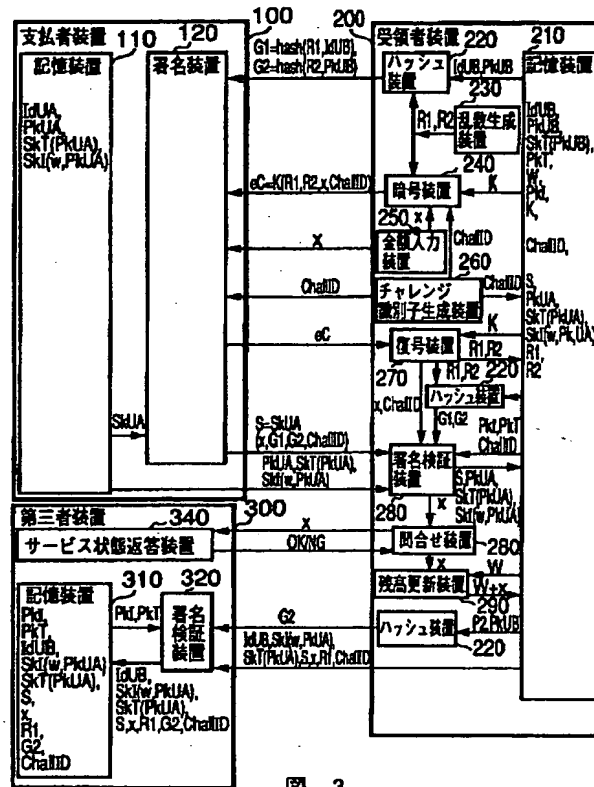


図 3

フロントページの続き

(51)Int. Cl.<sup>7</sup>

識別記号

F I  
G 0 7 F 7/08

テマコード(参考)

J

Fターム(参考) 3E040 AA03 CA12 DA02  
 3E044 BA04 CA06  
 5B055 CB08 CB09 CC16 EE29 HA12  
 KK05 KK16  
 5B058 KA35 KA40 YA20  
 9A001 BZ03 EE03 JJ66 JJ67 LL03